(L16) (April 20, 2020 (!)) To continue, we show that for an ideal $I \subset R$ in a ring R, the operations $+$ and $\cdot$ on the factor-ring R/I are well defined, as their results do not depend on selection of representatives of the factor classes $\{a+I \mid a \in R\}$. So let $a+I = a'+I$ and $b+I = b'+I$ (where $a, a', b, b' \in R$). Thus $a-a', b-b' \in I$ and $(a+b)-(a'+b') = (a-a')+(b-b') \in I$, by the def. of ideals, and $(a+I)+(b+I) = (a'+I)+(b'+I)$. As for the product, $ab - a'b' = ab - (a+a'-a)(b+b'-b) =$

$= ab - a(b'-b) - (a'-a)b - (a'-a)(b'-b) \in I$

($-ab$: $\in I$; $a(b'-b)$: $\in I$; $(a'-a)b$: $\in I$; $(a'-a)(b'-b)$: $\in I$; $-ab - a(b'-b)$: $\in I$; $-(a'-a)b - (a'-a)(b'-b)$: $\in I$; all: $\in I$) — by the def. of ideals.

$= (a'+I)(b'+I)$

thus $ab+I = a'b'+I$.

$(a+I)(b+I)$ ☒

the most important result on ideals in rings, which we actually will need (to construct finite fields) is the following

Theorem (on R/I) Let R be a ring and $I \subsetneq R$ be an ideal. Then 1) I is a prime ideal $\Leftrightarrow$ R/I is an integral domain.

2) I is maximal $\Leftrightarrow$ R/I is a field.

Proof We denote $S = R/I$. 1) $\Rightarrow$ We assume that I is a prime ideal and have $a, b \in R$ s.t. $(a+I)\cdot(b+I) = ab+I = 0_S$, i.e. $ab \in I$. But then $a \in I$ or $b \in I \rightsquigarrow a+I = 0_S$ or $b+I = 0_S$ and S is an integral domain. $\Leftarrow$ We assume that S is an i.d. and have $a, b \in R$ with $ab \in I$. Thus $ab+I = 0_S \rightsquigarrow a+I = 0_S$ or $b+I = 0_S$

$(a+I)\cdot(b+I)$

and $a \in I$ or $b \in I$. thus I is a prime ideal.

2) $\Rightarrow$ We assume that I is maximal and have an $a+I \in S$, $a+I \neq 0_S$. this

means that $a \in R \setminus I$. ~~the smallest ideal~~ ~~containing~~ the set

$\exists \subseteq R$ ~~that contains~~ $= \{x + ra \mid x \in I, r \in R\}$ is an ideal —

Problem 16.1 Prove it. — but $\exists \neq I$

(because $x + 0_R a \in \exists$ and $0_R + 1_R a = a \in \exists$)

(and by the maximality of I we get that $\exists = R$. thus $1_R \in \exists$ and $\exists x \in I \; \exists r \in R$ s.t. $x + ra = 1_R \rightsquigarrow 1_R - ra \in I$ and $(r+I) \cdot (a+I) = ra + I =$

$= 1_R + I = 1_S$ and $a+I$ is invertible in S.

(thus S is a field.

Problem 16.2 this I forgot to prove: $0_R + I$ is neutral to $+$ in the factor-ring R/I and similarly $1_R + I$ is 1_S.

Prove it. $\Leftarrow$ We assume that $S = R/I$ is a field and have an element $a \in R \setminus I$. then ($a + I \neq 0_S$ and there is an element $b + I \in S$ s.t. $(a+I)(b+I) = ab + I = 1_S = 1_R + I$.

$\rightsquigarrow \exists c \in I : ab = 1_R + c$. Now if $J \subseteq R$ (4) is an ideal s.t. $I \subsetneq J$, we can take such an $a \in J \setminus I$ and get that $1_R = ab - c$ for some $b \in R$ and $c \in I$, thus $1_R = \underbrace{\underbrace{ab}_{\in J} - \underbrace{c}_{\in J}}_{\in J} \in J$. But this means that $J = R$.

thus I is a maximal ideal. ☒

We still need - for the construction of a finite field with p^2 elements - ~~one~~ two more general results on rings. Let R be an integral domain. **Definition** We say that R is a PID (principal ideal domain), also Pražská (integrovaná doprava) if $\forall$ ideal $I \subseteq R$ is principal, is generated by a single element a, i.e. has form $I = \langle \{a\} \rangle = \{ra \mid r \in R\}$ (*), $a \in R$.

Proposition Let F be a field and $R = F[x] = \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in F, n \in \mathbb{N}_0\}$ be

the ring of polynomials with coeff-s in F.
(then $F[x]$ is a PID. Proof.

Problem 16.3 Prove that $F[x]$ is an integral domain. Does it hold if we assume only that F is an integral domain? So

($F[x]$ is an i.d. and we take an ideal $I \subseteq F[x]$, $I \neq \{0_R\}$ ($\{0_R\}$ is trivially principal) and a polynomial $a(x) \in I$ s.t. $a(x) \neq 0$ and $\deg(a)$ is minimum. We claim that a divides every $b \in I$ and so $I = \langle \{a\} \rangle = a(a)$.

(this follows simply from dividing b by a with residue c: $b = da + c$ where $d \in F[x]$, $c = 0_R$ or $\deg(c) < \deg(a)$. But this is impossible as $c = b - da \in I$. thus $c = 0_R$ (and $a \mid b$. $\in I$ $\in I$

-) the principal ideal $\langle \{a\} \rangle$ is denoted (a). ☒

Definition An element $a \in R$[1] in an integral domain R is called <u>irreducible</u> if $a = bc$ with $b, c \in R$ implies that b or c is a unit in R (i.e. is invertible).

Proposition Suppose that R is a PID and $a \in R$ is irreducible. Then the ideal (a) is maximal.

Proof: Let $I \subseteq R$ be an ideal with $I \supseteq (a)$. Thus $I = (b)$ for some $b \in R$. From $I \supseteq (a)$ we get that $a \in (b)$ and so $a = bc$ for some $c \in R$. Thus c is a unit, then $b = ac^{-1} \in (a)$ and $I \subseteq (a)$ and $I \neq (a)$, or b is a unit, then $1_R \in I$ and $I = R$. Thus (a) is maximal. ☒

I see that we in fact need yet one more general result – that $\forall$ field F the ring $F[x]$ is a UFD (unique factorization domain) – but more on this next time.

---

1) s.t. $a \neq 0_R$ and a is not a unit in R.